SSG L2TP Dial-Out

The SSG L2TP Dial-Out feature enhances SSG tunnel services and provides a dial-out facility to users. Many small offices/home offices (SOHOs) use the public switched telephone network (PSTN) to access their intranets. SSG L2TP provides mobile users with a way to securely connect to their SOHOs through the PSTN. SSG L2TP Dial-Out also provides a convenient way for general packet radio service (GPRS) users to connect to their SOHOs.

Feature History for the SSG L2TP Dial-Out Feature

Release	Modification
12.2(15)B	This feature was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for SSG L2TP Dial-Out

SSG L2TP Dial-Out does not support the following functionality:

- Layer 2 Tunneling Protocol (L2TP) dial-out as a primary service for PPP users
- Challenge Handshake Authentication Protocol (CHAP) authentication for dial-out tunnel services
- A single user connecting to two overlapping services
- Dial-out tunnels support for protocols other than L2TP protocols

Information About SSG L2TP Dial-Out

To configure the SSG L2TP Dial-Out feature, you should understand the following concepts:

Overview of SSG

Service Selection Gateway (SSG) is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

For more information about SSG, see the "Additional References" section on page 24.

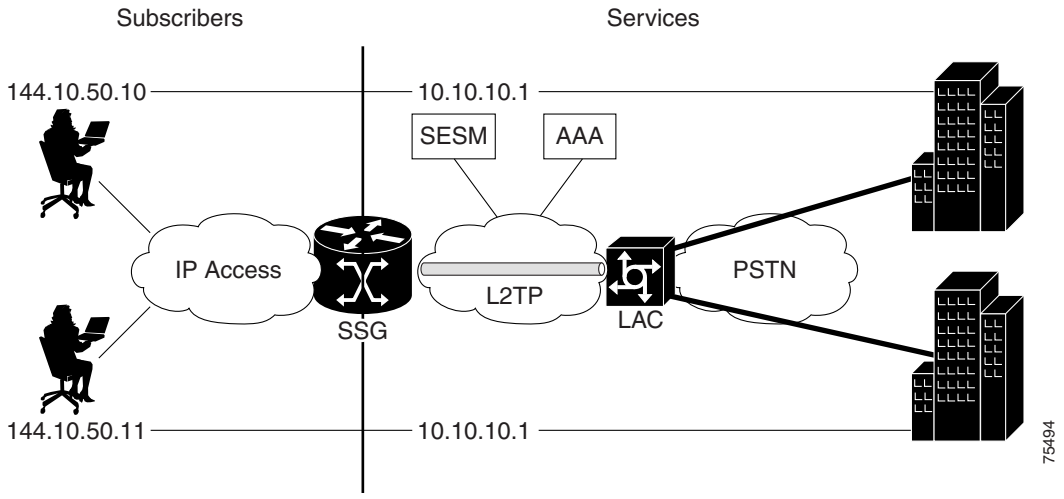
SSG L2TP Dial-Out

The SSG L2TP Dial-Out feature provides mobile users with a way to securely connect to their SOHOs through the PSTN.

To provide SSG L2TP Dial-Out, SSG requires a digital number identification service (DNIS) number for the SOHO to which the user wants to connect, the address of the L2TP Access Concentrator (LAC) closest to the SOHO, and configured tunnel parameters to establish a tunnel to the LAC.

Users can access SSG L2TP Dial-Out by selecting the dial-out service using Cisco Subscriber Edge Services Manager (SESM) from the list of subscribed services or by using a structured username. The user must provide the DNIS number when using either method of connecting to the dial-out service.

Figure 1 SSG L2TP Dial-Out Network



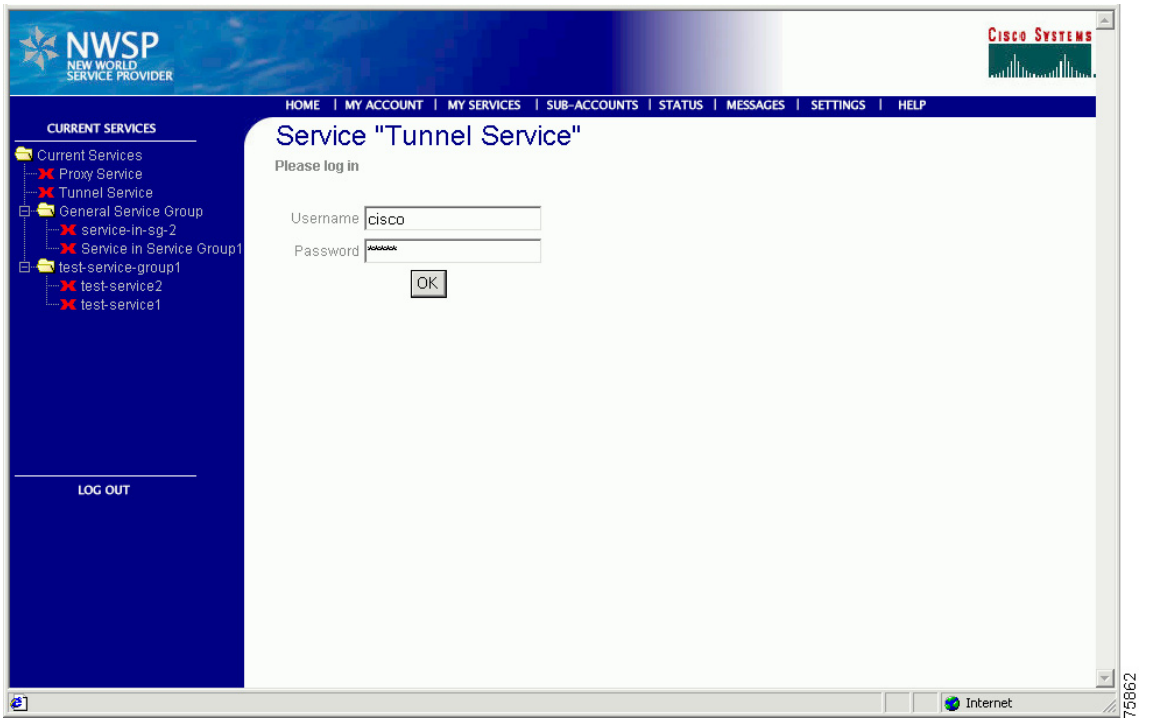
SSG L2TP Dial-Out Service Logon Through SESM

A user can access SSG L2TP Dial-Out by selecting the dial-out tunnel service (shown as Tunnel Service) on the SESM.

Figure 2 Sample SESM Welcome Page

After a user selects the dial-out service, the SESM displays a page for the entry of the user's name and password. SSG then downloads the service profile for the dial-out service.

Figure 3 Sample SESM User-Logon Screen

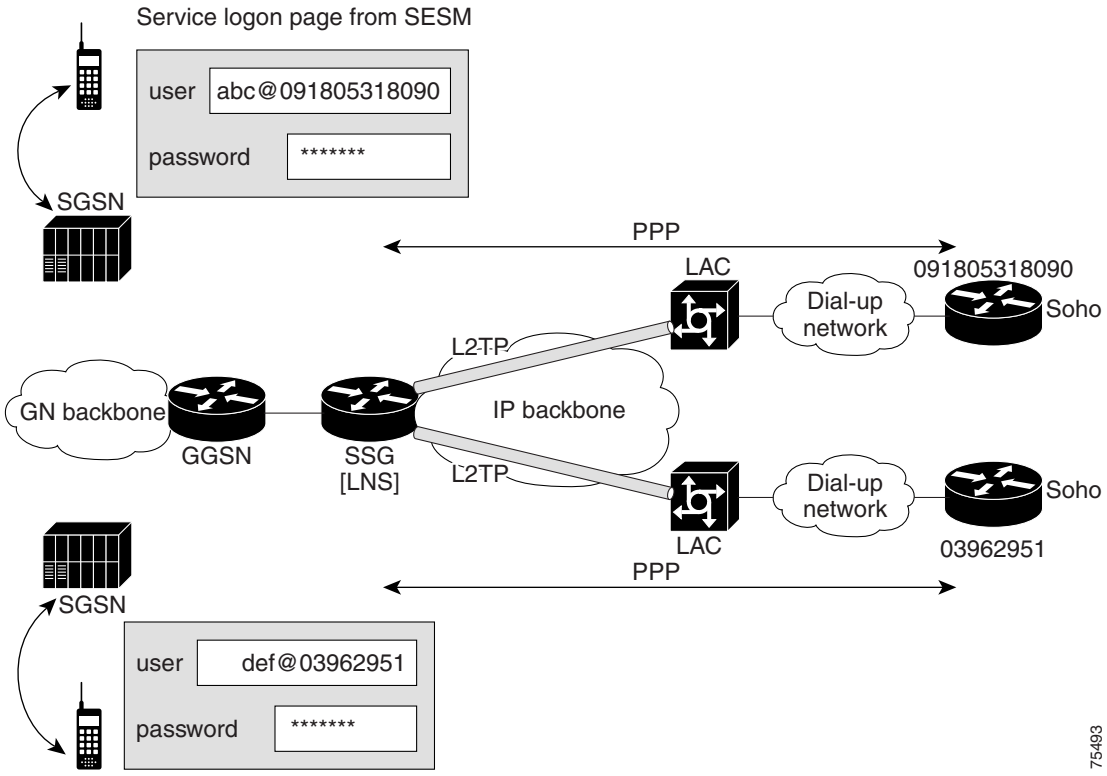


When a user attempts to log on to a dial-out service, the username entered into the SESM must have a numerical realm that is a DNIS prefix; for example, abc@091805318090. If the DNIS prefix that the user enters is found on the DNIS exclusion list, the logon is rejected. If the entered DNIS prefix is valid, a tunnel session to the LAC is established, and SSG starts PPP negotiations with the SOHO. The user is then authenticated at the SOHO.

If you configure the X attribute in the service profile, the full username (abc@091805318090) is sent for authentication. Otherwise, only the username (abc) is authenticated.

Upon successful authentication, the SOHO assigns an IP address to the user, and Network Address Translation (NAT) for the assigned IP address is performed in SSG.

Figure 4 SSG L2TP Dial-Out Service Logon Through SESM



SSG L2TP Dial-Out Service Account Logon with Structured Username and Without SSG Autodomain

When a user attempts an account logon with a structured username and the SSG Autodomain feature is not enabled, the entered username is sent to a local authentication, authorization, and accounting (AAA) server for user authentication. If the username entered is a structured username, SSG does not interpret the full username as user and domain. If the username is entered as "user@DNIS", the full username is used for user authentication.

If a user has a dial-out tunnel service configured as an autologon service and does not specify a username and password along with the service name in the user profile, the username and password entered for account logon are used. If the username and password are given with the service name in the user profile, then that username and password are used. The username entered in either case must be "user@DNIS". The DNIS portion of the username is used as the dial string to dial from the LAC to the SOHO.

SSG L2TP Dial-Out Service Logon with Structured Username and with SSG Autodomain

To enable users to access the dial-out service at the time of account logon, you must configure a static service profile with the LAC address. When users log on as "user@DNIS", the user is connected to the SOHO via the LAC configured in the service profile.

When the SSG Autodomain feature is enabled, a full username must be entered by the user at the account logon page if the user wants to perform service selection by using the DNIS number. SSG interprets the full username as username and domain. For "user@DNIS", "user" is the username and "DNIS" is the domain. This "DNIS" domain must be a numerical value; for example, "user@3962962."

You can select the dial-out global service that is available to a user who performs an account logon with a structured username (user@DNIS) by configuring the **dnis-prefix all service** command.

SSG Autodomain Basic and Extended Modes

You can configure SSG Autodomain in basic or extended mode. In basic mode, the SSG Autodomain profile downloaded from the AAA server is a service profile. In extended SSG Autodomain mode, the SSG Autodomain profile downloaded from the AAA server is a "virtual-user" profile. In the virtual-user profile, the dial-out service is configured as the primary autologon service.

When SSG Autodomain is configured, SSG parses the structured username. If the domain part of the username is a DNIS prefix, the SSG Autodomain profile is downloaded. You can configure the SSG Autodomain profile by configuring the **dnis-prefix all service** command. If the SSG Autodomain profile has not been configured or the DNIS prefix is included in the DNIS exclusion list, the account logon is rejected.

If the account logon is successful and the configured service is a dial-out service, SSG establishes a tunnel session with the LAC. The IP address of the LAC must be configured in the SSG Autodomain profile. SSG uses the DNIS number that was entered as part of the username as the dial string to dial out to the SOHO from the LAC. When the PPP session begins successfully, the user is authenticated at the SOHO. If the X attribute is configured in the SSG Autodomain profile, the full username is sent for authentication.

SSG performs Network Address Translation (NAT) for the user's IP address for a tunnel by default. If you enter the **no nat user-address** command when SSG Autodomain is configured, SSG does not perform NAT on the user's IP address. The IP address assigned to the SOHO is assigned to the user.

For more information about the SSG Autodomain feature, see the "Additional References" section on page 24.

MSISDN with DNIS

You can configure the service profile to send the mobile station integrated services digital network (MSISDN) number along with the DNIS number to the SOHO. By default, only the DNIS number is sent while the dial-out tunnel is being established. When the MSISDN/DNSI vendor-specific attribute (VSA) is present in the service, the MSISDN/DNIS dial string takes the following format:

DNIS-*number_delimiter* MSISDN-*number*

The delimiter can be any regular expression character (A, B, C, D, 0–9, #, *,\, $,., ^) that is not in the DNIS or in the MSISDN number. If you do not specify a delimiter, the "@" character is the default delimiter.

If there is no MSISDN for the subscriber, only the DNIS number is sent as the dial string.

Table 1 MSISDN/DNIS VSA

Attribute ID	Vendor ID	Subattribute ID and Type	Attribute Name	Subattribute Data
26	9	251	MSISDN/DNIS	Y—Service-information code for sending MSISDN with DNIS G—Delimiter character that separates the DNIS number from the MSISDN number.

DNIS Filters

To block PSTN calls to unwanted DNIS numbers, such as free phone or international numbers, you can configure a DNIS filter. DNIS filters can be locally configured through the command line interface (CLI) or received from a AAA profile. Use the **exclude dnis-prefix** command in SSG dial-out configuration mode to configure a DNIS filter locally. Use the **download exclude-profile (ssg dial-out)** command in SSG dial-out configuration mode to download a DNIS filter from the AAA server. To configure a DNIS filte,r see the ""Configuring a DNIS Filter" section on page 10.

SSG L2TP Dial-Out As an Autologon Service

You can configure dial-out tunnel service as an autologon service. To configure a tunnel service as an autologon service, configure the username and password within the service profile, for example;

```
}
reply_attributes={
9,250="Adial-out-tunnel_service;user@DNIS;cisco"
}
```

If the username and password are not configured within the service profile, SSG uses the username and password entered during account logon for authentication.

Service Logoff

When a user logs on to a dial-out tunnel service by selecting it from the service page of SESM, and then logs off from that service, the connection to the service is removed.

If the dial-out tunnel service is an Autodomain primary service, and the user logs off from the dial-out tunnel service, the user is also logged off from all other services.

Dial-Out Service Identification

When you configure the service profile for a dial-out tunnel service, configure the same parameters that are used for dial-in tunnel service, along with the additional Cisco attribute value (AV) pair "vpdn:dout-type=2" in the user profile. The 2 represents the L2TP protocol. Only the L2TP protocol is supported for dial-out tunnels.

Overlapping IP Addresses

SSG L2TP Dial-Out supports overlapping user addresses only on routed point-to-point interfaces in host-key mode. If the Host Key feature is not enabled, SSG does not support overlapping users. Even with the Host Key featured enabled, a single user cannot connect to two overlapping services.

For more information about SSG in host-key mode, including configuration information, see the "Additional References" section on page 24.

How to Configure SSG L2TP Dial-Out

This section contains the following procedures:

Configuring a Global Dial-Out Service Profile

Perform this task to configure a global dial-out service profile.

For more information about configuring service profiles, see the "Service Profiles" section of the Service Selection Gateway new-feature document for Cisco IOS Release 12.2(8)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg enable**
4. **ssg dial-out**
5. **dnis-prefix all service** *service-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG functionality.
Step 4	**ssg dial-out** **Example:** `Router(config)# ssg dial-out`	Enters SSG dial-out configuration mode. **Note** There is no command to enable or disable the SSG L2TP Dial-Out feature. An L2TP dial-out tunnel is established if the service profile contains the "vpdn:dout-type=2" attribute.
Step 5	**dnis-prefix all service** *service-name* **Example:** `Router(config-dial-out)# dnis-prefix all service service1`	Configures the dial-out global service name. The global service is configured for users who are doing an account logon with a structured username. • *service-name*—Name of the dial-out global service.

Configuring the User Service Profile

Service profiles include password, service type (outbound), type of service (tunnel), service access mode (sequential or concurrent), DNS server IP address, networks that exist in the service domain, access control lists, and other optional attributes.

To configure the service profile for users when SSG Autodomain is configured in basic mode, configure the IP address of the LAC in the user service profile.

For SSG Autodomain configured in extended mode, the service profile is a virtual-user profile with dial-out tunnel service configured as a primary service.

To configure the dial-out tunnel service to be an autologon service, the username and password must be configured with the service name attribute for tunnel service. This attribute subscribes the user to a service and automatically logs the user on to the service. The user profile attribute has the following syntax:

Account-Info = "**A***servicename* [;*username*;*password*]"

servicename	Name of the service.
username	Username used to access the service. Required for proxy services and tunnel services.
password	Password used to access the service. Required for proxy services and tunnel services.

Each user profile can have more than one autoservice attribute.

To enable SSG L2TP Dial-Out, the service profile must contain the following attribute:

”vpdn:dout-type=2”

To send the MSISDN with DNIS while establishing the dial-out tunnel, the service profile must contain the Y attribute.

Configuring a DNIS Filter

Perform this task to configure a DNIS filter.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg dial-out**
4. **exclude dnis-prefix** *dnis-prefix*
5. Repeat Step 3 to add DNIS prefixes to the DNIS exclusion list.
6. **download exclude-profile** *profile-name password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ssg enable** **Example:** `Router(config)# ssg enable`	Enables SSG functionality.
Step 4	**ssg dial-out** **Example:** `Router(config)# ssg dial-out`	Enters SSG dial-out configuration mode.
Step 5	**exclude dnis-prefix** *dnis-prefix* **Example:** `Router(config-dial-out)# exclude dnis-prefix 18085288110`	(Optional) Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list. • *dnis-prefix*—The DNIS prefix to add to the DNIS exclusion list.

	Command or Action	Purpose
Step 6	(Optional) Repeat Step 3 to add DNIS prefixes to the DNIS exclusion list.	
Step 7	**download exclude-profile** *profile-name password* **Example:** `Router(config-dial-out)# download exclude-profile profile_1 cisco`	(Optional) Downloads the DNIS exclusion list locally or from AAA. • *profile-name*—Name of the DNIS exclusion list. • *password*—Password of the DNIS exclusion list.

Verifying SSG L2TP Dial-Out

Perform this task to verify configuration of SSG L2TP Dial-Out.

SUMMARY STEPS

Step 1 **show ssg host**

Step 2 Select "L2TP Dial-Out" service from the list.

Step 3 Enter the username (john@dnis) and password when prompted.

Step 4 **show ssg service**

Step 5 **show ssg connection** *user-ip service-name*

Step 6 **ping** *ip-address*

DETAILED STEPS

Step 1 **show ssg host**

Enter this command to verify that user logon is successful.

```
Router# show ssg host

1: 60.0.0.2 !IP address of the user.
### Active HostObject Count: 1
```

Step 2 If the user logon is successful, the user sees a new page that displays the subscribed services. Select "L2TP Dial-Out" service from the list.

Step 3 The user is prompted for the service logon. Enter the username (john@dnis) and password. This prompts SSG to create a tunnel to the LAC. The LAC dials out to the SOHO, and the connection is established.

Step 4 **show ssg service**

Enter this command to verify that the service logon is successful.

```
Router# show ssg service

1: soho0

### Total ServiceInfoObject Count: 1
```

Step 5 **show ssg connection** *user-ip service-name*

Enter the **show ssg connection** *user-ip service-name* command to verify that the LAC connection to the SOHO is successful.

```
Router# show ssg connection 60.0.0.2 soho0

-----------------------ConnectionObject Content -----------------------
User Name: john
Owner Host: 60.0.0.2
Associated Service: soho0
DNIS number = 4444007
Connection State: 0 (UP)
Connection Started since: *14:42:50.000 UTC Mon Mar 1 1993
Connection Real IP: 5.0.0.20
L2TP VIDB: Virtual-Access5
User last activity at: *14:42:51.000 UTC Mon Mar 1 1993
Connection Traffic Statistics:
        Input Bytes = 0, Input packets = 0
        Output Bytes = 0, Output packets = 0
Session policing disabled
```

Step 6 **ping** *ip-address*

Send a ping from the service to the user network to verify connection.

```
Router# ping 60.0.0.2
```

Troubleshooting SSG L2TP Dial-Out

Verify that the configurations for the routers and AAA have loaded successfully by entering the **show running-config** command. Confirm that your output matches the configuration examples shown in the "Configuration Examples" section on page 14.

Troubleshooting User Logon Failures

- Enter the **debug ssg ctrl-events** command.

  ```
  Router# debug ssg ctrl-events

  SSG-CTL-EVN: AAA Response is bad
  .
  .
  .
  SSG-CTL-EVN: Failed to get user info. user=dt-user90, pwd=*****
  ```

  If either of the two outputs above is displayed, the user profile does not exist, the password is incorrect in AAA, or the AAA is not configured. Enable AAA by entering the **aaa new-model** command.

- Enter the **debug ssg radius** command.

  ```
  Router# debug ssg radius

  RADIUS: No radius servers defined!
  ```

  The output above is displayed if the RADIUS server is not configured or is not reachable.

  Configure the RADIUS server by entering the following command:

  ```
  Router# radius-server host 10.0.0.0 auth-port 1645 acct-port 1646
  ```

  If the **debug ssg radius** command displays the following output, there is a RADIUS server key mismatch:

  ```
  RADIUS: Response (159) failed decrypt
  ```

Enter the **radius-server key ssg** command to configure the correct key.

- Enter the **debug ssg ctrl-err** command.

```
Router# debug ssg ctrl-err

SSG-CTL-ERR: Unable to find SSG sub-block from ATM3/0.1
```

The output above indicates that the ATM3/0.1 interface, where the user is coming from, is not configured as a downlink interface. SSG requires that all the interfaces to the subscribers be bound as downlink interfaces.

Enter the **ssg direction downlink** command in interface configuration mode to configure the interface as downlink.

Troubleshooting Service Login Failures

- Enter the **debug ssg ctrl-events** command.

```
Router# debug ssg ctrl-events

SSG-CTL-EVN: Invalid DNIS number for dialout tunnel service
```

The output above indicates that an invalid DNIS number has been configured. The DNIS number should be configured according to the E.165 standard. Valid DNIS numbers can contain the following characters: A, B, C, D, 0–9, #, *, and ., and they can start with +, and end with T .

Any issues on the LAC or SOHO side will cause the following outputs in the **debug ssg ctrl-events** command:

```
SSG-VPDN-CTL-EVN: VPDN module failed to establish tunnel

or
SSG-VPDN-CTL-EVN: Failed to establish call..informing SSG
```

Follow the steps below to troubleshoot this problem:

Step 1 After giving the service logon request, enter the **show vpdn tunnel** command to view the tunnel status (the tunnel will time out after some time.)

Step 2 If the tunnel has come up, skip this step. If the tunnel is not up, enable the **debug vpdn l2x-events** and **debug vpdn l2x-errors** commands on the SSG and on the LAC.

Common problems are tunnel ID mismatch and destination IP not reachable.

Step 3 Once the tunnel is up, problems can appear on the dialer interface.

- Enable **debug ppp negotiation** and **debug ppp authentication** commands.
- If no PPP debug messages are seen, it is confirmed that the problem is with the dialer interface.

Step 4 Enable the **debug dialer** and **debug isdn q921, 931** commands on the LAC and on the SOHO. A common problem is ISDN status “not established.”

For Dialer interface configuration problems, cut and paste the configuration given in the “Configuration Examples” section on page 14 again and look for any command rejections. Most problems will have to do with ISDN (Layer 2). If the ISDN status is not established, reload the LAC or SOHO.

Common problems found in the PPP debug messages are: authentication failed and IPCP negotiation failed.

Monitoring and Maintaining SSG L2TP Dial-Out

Perform this task to monitor and maintain the SSG L2TP Dial-Out feature.

SUMMARY STEPS

1. **enable**
1. **show ssg dial-out exclude-list**
2. **show ssg service** [*service-name*]
3. **show ssg connection** *ip-address service-name* [*interface*]

DETAILED STEPS

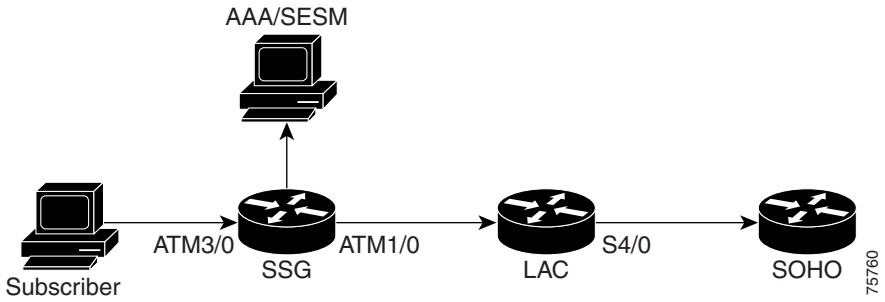
	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ssg dial-out exclude-list** **Example:** `Router# show ssg dial-out exclude-list`	Displays information about the DNIS exclusion list.
Step 3	**show ssg service** [*service-name*] **Example:** `Router# show ssg service service1`	Displays detailed information about a service. If no service name is entered, this command displays a list of all services. • *service-name*—(Optional) Name of an active SSG service.
Step 4	**show ssg connection** *ip-address service-name* [*interface*] **Example:** `Router# Router# show ssg connection 10.1.1.19 InstMsg`	Displays the connections of a given host and a service name. • *ip-address*—IP address of an active SSG connection. This is always a subscribed host. • *service-name*—Name of an active SSG connection. • *interface*—(Optional) The IP address through which the host is connected.

Configuration Examples for SSG L2TP Dial-Out

Configuring SSG L2TP Dial-Out for SSG Without SSG Autodomain Enabled: Example

The following example shows the minimum configurations needed for an SSG L2TP Dial-Out solution for an SSG with SSG Autodomain disabled, one LAC and one SOHO. Figure 5 illustrates a sample SSG L2TP Dial-Out network.

Figure 5 Sample SSG L2TP Dial-Out Network



In this configuration, the SSG user can access the SOHO in two ways, with an account logon and then a service logon or with an account logon with service configured as an autologon service.

User Profile Configurations

Use the following profile configuration when the SSG user accesses the SOHO with an account logon and then a service logon:

```
user=abc {
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,250-"Nsoho0"
}
}
}
```

Use the following profile configuration when the SSG user accesses the SOHO with an account logon with service configured as an autologon service:

```
user=abc {
radius-6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,250-"Asoho0;user@DNIS;cisco"
}
}
}
```

Service Profile Configuration

The following example shows how to configure the service profile:

```
user=soho0 {
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,251= "TT"
9,251="R172.0.0.1:255.0.0.0" ! This is the service network.
9,1="vpdn:ip-address=172.16.0.0"
9,1="vpdn:l2tp-tunnel-password=lab:
9,1=-"vpdn:tunnel-type=l2tp"
9,1="vpdn:tunnel-id=lns_l2x0"
9,1="vpdn:dout-type=2"
```

SSG Configuration

```
hostname SSG
aaa new-model
aaa authentication ppp default group radius
!
ip cef
vpdn enable
!
ssg enable
ssg default-network 10.1.1.1 255.255.255.255
ssg service-password cisco
ssg radius-helper auth-port 1645 acct-port 1646
ssg radius-helper key cisco
ssg bind direction downlink ATM3/0.1
1
interface ATM1/0.1 point-to-point ! For an IP user.
ip address 172.16.0.0 255.0.0.0
no ip mroute-cache
ip nat inside
pvc 0/33
!
interface ATM3/0.10 point-to-point ! For a PPP user.
pvc 0/100
encapsulation aal5mux ppp Virtual-Template1
!
interface Virtual-Template1
ip unnumbered Ethernet2/2
peer default ip address pool ppp_pool_1
ppp authentication pap
ip nat inside
!
radius-server host 10.2.36.253 auth-port 1645 acct-port 1646 timeout 5
radius-server retransmit 3
radius-server key ssg
ip local pool ppp_pool_1 10.0.0.1 10.0.0.255
```

LAC Configuration

```
hostname LAC
vpdn enable
vpdn-group 1
accept-dialout
 protocol l2tp
 dialer 0 ! Matches rotary group and the dialer interface.
terminate-from hostname lns_l2x0
l2tp tunnel password 7 abcdef
```

```
!
idsn switch-type primary-5ess
!
interface Dialer0 ! All users coming to VPDN-group 0 are handled by this interface.
no ip address
encapsulation ppp
dialer in-band
dialer aaa
ppp authentication pap
!
dialer-list 1 protocol ip permit
```

SOHO Configuration

```
hostname soho0
username john password 0 cisco
username john@1234567 password 0 cisco
!
controller T1 1/0
framing esf
linecode b8zs
pri-group timeslots 1-24
!
interface Serial1/0:23
 no ip address
 encapsulation ppp
 dialer rotary-group 0 ! This matches the interface Dialer0.
 isdn switch-type primary-5ess
 no peer default ip address
 no cdp enable
!
interface Dialer0
 ip unnumbered Loopback2
 encapsulation ppp
 dialer-group 1
 peer default ip address pool soho_1
 no cdp enable
 ppp authentication chap
!
ip local pool soho_1 10.0.0.20 10.0.0.40
dialer-list 1 protocol ip permit
```

Configuring SSG L2TP Dial-Out for SSG with SSG Autodomain Enabled: Example

The following example shows the minimum configurations needed for an SSG L2TP Dial-Out solution for an SSG with SSG Autodomain enabled, one LAC and one SOHO.

In this configuration, the SSG user can access the SOHO in two ways, with an account logon and then a service logon or with an account logon with “user@dnis” as the username. In this solution, services are selected based on the SSG Autodomain configuration and the global service configured in the SSG dial-out mode.

User Profile Configuration

When SSG Autodomain is enabled and the user accesses the SOHO with an account logon and then a service logon, you do not need to configure a service profile.

Use the following profile configuration when the SSG user accesses the SOHO with an account logon with “user@dnis” as the username:

```
user=soho1{
radius=6510-SSG-v1.1{
check_items= {
2=cisco
}
reply_attributes={
9,250="Asoho0"
9,250-"Npassthru1"
}
}
}
```

SSG Configuration

```
.
.
.
!
ssg dial-out
 dnis-prefix all service soho1 ! This indicates SSG Autodomain in extended mode.
```

or

```
 dnis-prefix all service soho0 ! This indicates SSG Autodomain in basic mode.
.
.
.
```

LAC and SOHO Configurations

The LAC and SOHO configurations for SSG with SSG Autodomain configured are the same as the configuration for SSG without SSG Autodomain enabled. See the "Configuring SSG L2TP Dialout for SSG without SSG Autodomain Enabled: Example" section on page 14 for more details.

Configuring User-Specific Configurations on the SOHO: Example

The following example shows how to configure user-specific configurations on the SOHO. The user profile, service profile, SSG, and LAC configurations are the same as in the "Configuring SSG L2TP Dialout for SSG without SSG Autodomain Enabled: Example" section on page 14.

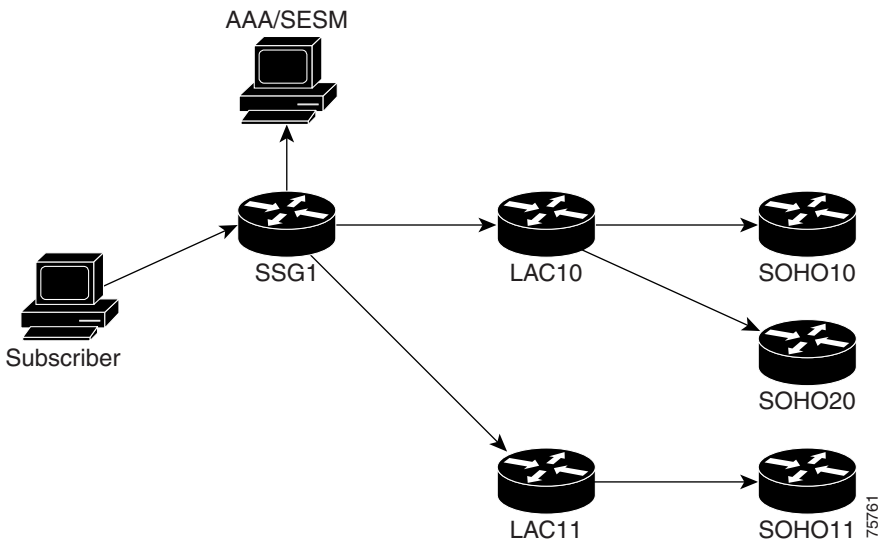
```
hostname soho0
username john password 0 cisco
username john@4444007 password 0 cisco
username Gary password cisco
!
controller t1 1/0
framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface serial1/1:23
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type primary-5ess
 no peer default ip address
 no cdp enable
 ppp authentication chap
!
interface Dialer1 ! Configures a special service policy and pool for user "john."
 ip unnumbered loopback1
 encapsulation ppp
 dialer pool 1
```

```
 dialer remote-name john
 dialer idle-timeout 2147483
 dialer string 3456048
 dialer-group 1
 service-policy output SETDSCP
 peer default ip address pool soho_1
!
interface Dialer2 ! Configures a special service policy and pool for user "gary."
 ip unnumbered loopback1
 encapsulation ppp
 dialer pool 1
 dialer remote-name gary
 dialer idle-timeout 2147483
 dialer-group 1
 peer default ip address pool soho_OLAPP
 pulse-time 0
 ppp authentication chap
!
ip local pool soho_1 10.0.0.20 10.0.0.40
ip local pool soho_OLAP 11.0.0.10
```

Configuring a Large-Scale SSG L2TP Dial-Out Solution: Example

The following example shows how to configure an SSG L2TP Dial-Out solution with multiple LACs and multiple SOHOs. Figure 6 shows a sample large-scale SSG L2TP Dial-Out network:

Figure 6 Sample Large-Scale SSG L2TP Dial-Out Network



User Profile Configuration

The user profile configuration is the same as that shown in the Configuring SSG L2TP Dial-Out for SSG Without SSG Autodomain Enabled: Example, page 15.

Service Profile Configuration

SSG selects the LAC to which it will create a tunnel by looking at the service profile. In the following example, the IP addresses configured in the LAC interfaces to SSG are

- LAC10 = 172.16.0.0
- LAC11 = 172.17.0.0

```
user = soho10{
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,251="TT"
9,251="R170.0.0.1;255.0.0.0"
9,1="vpdn:ip-addresses=172.16.0.0" ! IP address of LAC10.
9,1="vpdn:l2tp-tunnel-password=lab"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:tunnel-id=lns_l2x0"
9,1="vpdn:dout-type=2"
}
}
}

user = soho11{
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,251="TT"
9,251="R170.0.0.1;255.0.0.0"
9,1="vpdn:ip-addresses=172.17.0.0" ! IP address of LAC11.
9,1="vpdn:l2tp-tunnel-password=lab"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:tunnel-id=lns_l2x0"
9,1="vpdn:dout-type=2"
}
}
}
```

SSG Configuration

The SSG Configuration for a large-scale SSG L2TP Dial-Out solution is the same as that in the "Configuring SSG L2TP Dial-Out for SSG Without SSG Autodomain Enabled: Example" section on page 15.

LAC Configuration

The following example shows a sample configuration for LAC10:

```
hostname LAC10
vpdn enable
!
vpdn-group 1
accept-dialout
 protocol l2tp
  dialer 0 ! This configuration matches with rotory-group and dialer interfaces.
terminate-from hostname ForSoho10 ! This tunnel ID "ForSoho10" will be terminated.
l2tp tunnel password 7 060A0E23
!
vpdn-group 1
accept-dialout
```

```
 protocol l2tp
 dialer  1 ! To match with rotary-group and dialer interfaces.
terminate-from hostname ForSoho20 ! This tunnel ID "ForSoho20" will be terminated.
l2tp tunnel password 7 060A0E23
!

isdn switch-type primary-5ess
!
controller T1 4/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface ATM2/0.1 point-to-point
 ip address 100.0.0.2 255.0.0.0
 pvc 0/100
 !
interface Serial4/0:23
 no ip address
 encapsulation ppp
 dialer rotary-group 0
 dialer-group 1
 isdn switch-type primary-5ess
!
interface Dialer0
 no ip address
 encapsulation ppp
 dialer in-band
 dialer aaa
 ppp authentication pap
!
interface Serial4/1:23
 no ip address
 encapsulation ppp
 dialer rotary-group 1
 dialer-group 1
 isdn switch-type primary-5ess
!
interface Dialer1
 no ip address
 encapsulation ppp
 dialer in-band
 dialer aaa
 ppp authentication pap
!
dialer-list 1 protocol ip permit
```

SOHO Configuration

The SOHO configuration for a large-scale SSG L2TP Dial-Out solution is the same that as shown in the "Configuring SSG L2TP Dial-Out for SSG Without SSG Autodomain Enabled: Example" section on page 15.

Configuring a Global Dial-Out Service Profile: Example

The following example shows how to configure a global dial-out service profile called "dialout_1":

```
ssg enable
ssg dial-out
 dnis-prefix all service dialout_1
```

Configuring the Service Profiles: Examples

The following is an example of a service profile when SSG Autodomain is configured in basic mode:

```
user = dialout_tunnel1{
member = SSG-DEV
radius = 6510-SSG-v1.1 {
check_items= {
2 = cisco
}
reply_attributes= {
                        9,251 = "TT"
                        9,251 = "R172.16.0.0;255.255.0.0;I"
                        9,1 = "vpdn:ip-addresses=10.0.0.1"
                        9,1 = "vpdn:l2tp-tunnel-password=cisco"
                        9,1 = "vpdn:tunnel-type = l2tp"
                        9,1 = "vpdn:tunnel-id = ssg1"
                        9,1 = "vpdn:dout-type=2"
```

The following is an example of a virtual-user service profile when SSG Autodomain is configured in extended mode:

```
user = virtual_user_dout{
member = SSG-DEV
radius=6510-SSG-v1.1{
check_items= {
2 = cisco
}
reply_attributes= {
                        9,251 = "Adial-out-tunnel_service"
                        9,251 = "Nproxynat_service"
                        9,250 = "Npassthru_service"
}
}
```

The following example shows how to configure a service profile with the SSG service-info VSA to send the MSISDN number along with DNIS number while establishing the dial-out tunnel.

The attribute 9,251="Y" sends the MSISDN number with the DNIS number. The character "#" is the delimiter between the DNIS number and the MSISDN number.

```
user = dialout_tunnel{
member=SSG-DEV
radius=6510-SSG-v1.1{
check_items= {
2=cisco
}
reply_attributes= {
9,251="TT"
9,251="R172.16.0.0;255.255.0.0;I"
9,1="vpdn:ip-addresses=10.0.0.0"
9,1="vpdn:l2tp-tunnel-password=cisco"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:tunnel-id=ssg1"
9,1="vpdn:dout-type:2"
9,251="Y#" ! MSISDN/DNIS attribute
```

Configuring a DNIS Filter: Examples

The following example shows how to configure a DNIS exclude profile in AAA:

```
user = exclude_dnis_aaa{
profile_id = 49
```

```
set server current-failed-logins = 0
profile_cycle = 25
member = SSG-DEV
radius=6510-SSG-v1.1 {
check_items= {
2=cisco
}
reply_attributes= {
9,253="XD+444"
9,253="XD22222T"
}
}
}
```

The following example shows how to add two DNIS prefixes to the exclude profile and to download a DNIS exclude profile named “profile_1” with a password of “cisco”:

```
ssg enable
ssg service-search-order local
ssg dial-out
 exclude dnis-prefix 18085288110
 exclude dnis-prefix 18085288111
 download exclude-profile profile_1 cisco
```

Additional References

The following sections provide references related to the SSG L2TP Dial-Out feature.

Related Documents

Related Topic	Document Title
SSG commands	*Cisco IOS Wide-Area Networking Command Reference*, Release 12.3 T
SSG configuration tasks	*Service Selection Gateway,* 12.3(4)T new-feature document
	Service Selection Gateway Accounting Update Interval per Service, 12.2(13)T new-feature document
	Service Selection Gateway Hierarchical Policing, 12.2(13)T new-feature document
	SSG AutoDomain, 12.2(13)T new-feature document
	SSG Autologoff Enhancement, 12.3(4)T new-feature document
	SSG Autologon Using Proxy Radius, 12.2(13)T new-feature document
	SSG Autologoff, 12.2(13)T new-feature document
	SSG Proxy for CDMA2000, 12.3(4)T new-feature document
	SSG Direction Configuration for Interfaces and Ranges, 12.3(4)T new-feature document
	SSG EAP Transparency, 12.3(4)T new-feature document
	SSG L2TP Dial-Out, 12.3(4)T new-feature document
	SSG Open Garden, 12.2(13)T new-feature document
	SSG Port-Bundle Host Key, 12.2(13)T new-feature document
	SSG Prepaid, 12.2(13)T new-feature document
	SSG Prepaid Idle Timeout, 12.3(4)T new-feature document
	SSG Service Profile Caching, 12.3(4)T new-feature document
	SSG Suppression of Unused Accounting Records, 12.3(4)T new-feature document
	SSG TCP Redirect for Services, 12.2(13)T new-feature document
	SSG Unconfig, 12.3(4)T new-feature document
	SSG Unique Session ID, 12.3(4)T new-feature document
SESM	*Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*
	Cisco Service Selection Dashboard Installation and Configuration Guide
	Cisco Service Selection Dashboard Web Developer Guide

Related Topic	Document Title
RADIUS commands	*Cisco IOS Security Command Reference*, Release 12.3 T
RADIUS configuration tasks	*Cisco IOS Security Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature. Support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature. Support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature. Support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents the following new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

- **dnis-prefix all service**

- download exclude-profile (ssg dial-out)
- exclude dnis-prefix
- show ssg dial-out exclude-list
- ssg dial-out

dnis-prefix all service

To configure the dial-out global service, use the **dnis-prefix all service** command in SSG dial-out configuration mode. To remove a service name and prevent further connections to the specified service, use the **no** form of this command.

dnis-prefix all service *service-name*

no dnis-prefix all service [*service-name*]

Syntax Description

service-name	Name of the dial-out global service.

Defaults

Dial-out global service is not configured.

Command Modes

SSG dial-out configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to configure the dial-out global service used for users who are doing account logon with a structured username (*user@DNIS*). The service profile is downloaded when the user connects to the dial-out service. You can specify only one dial-out global service. If you configure this command more than once and use different service names each time, the previously configured service name is removed from the configuration.

If SSG is operating in SSG Autodomain basic mode, you should configure the dial-out tunnel service profile as the dial-out global service. If SSG is operating in SSG Autodomain extended mode, you should configure the virtual-user profile as the dial-out global service and configure dial-out tunnel service as an Autologon service within SSG Autodomain extended mode.

Examples

The following example shows how to configure a global dial-out service profile named “profile1” as the global dial-out service profile:

```
dnis-prefix all service profile1
```

The following example shows how to configure a global dial-out service profile when SSG is operating in SSG Autodomain basic mode:

```
dnis-prefix all service dialout_tunnel
```

The following example shows how to configure a global dial-out service profile when SSG is operating in SSG Autodomain extended mode:

```
dnis-prefix all service virtual-user
```

Related Commands

Command	Purpose
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

download exclude-profile (ssg dial-out)

To download the Digital Number Identification Service (DNIS) exclusion list locally or from a authentication, authorization, and accounting (AAA) server, use the **download exclude-profile** command in SSG dial-out configuration mode. To remove the DNIS exclusion list from the configuration, use the **no** form of this command.

download exclude-profile *profile-name* [*password*]

no download exclude-profile *profile-name* [*password*]

Syntax Description

profile-name	Name of the DNIS exclusion list.
password	(Optional) Password of the DNIS exclusion list.

Defaults

A DNIS exclusion list is not downloaded.

Command Modes

SSG dial-out configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to download a DNIS exclusion list from the local profile configured in SSG or from a AAA server. If you do not specify a profile name and password, SSG attempts to download the profile with the previously configured profile name and password. If there is no previously configured profile name and password, the DNIS exclusion list is not downloaded.

You can download only one DNIS exclusion list. If you attempt to use the **download exclude-profile** command multiple times with different profile names, only the last profile name is downloaded and the previously downloaded profiles are removed from the configuration.

Use the **no download exclude-profile** command to remove the downloaded DNIS exclusion list from the configuration.

You can configure the order in which SSG searches for the DNIS exclusion list using the **ssg service-search-order** command.

Examples

The following example shows how to download a DNIS exclusion list with a profile name of "dnisprofile1" and a password of "abc":

```
download exclude-profile dnisprofile1 abc
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.
ssg service-search-order	Specifies the order in which SSG searches for a service profile.

exclude dnis-prefix

To configure the Digital Number Identification Service (DNIS) filter by adding a DNIS prefix to the DNIS exclusion list, use the **exclude dnis-prefix** command in SSG dial-out configuration mode. To remove a DNIS prefix from the DNIS exclusion list, use the **no** form of this command.

exclude dnis-prefix *dnis-prefix*

no exclude dnis-prefix *dnis-prefix*

Syntax Description

dnis-prefix	The DNIS prefix to be added to the DNIS exclusion list.

Defaults

No prefix is added

Command Modes

SSG dial-out configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to add a DNIS prefix to the DNIS exclusion list. You can use this command to add multiple DNIS prefixes to the DNIS exclusion list. When a user dials with a DNIS whose prefix is in the DNIS exclusion list, the service logon for that user is rejected.

Examples

The following example adds the DNIS prefix "1122334455" to the DNIS exclusion list:

```
exclude dnis-prefix 1122334455
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

show ssg dial-out exclude-list

To display information about the DNIS prefix profile and the DNIS exclusion list, use the **show ssg dial-out exclude-list** command in privileged EXEC mode.

show ssg dial-out exclude-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to display the DNIS profile name and all DNIS entries configured via CLI or downloaded from a AAA server.

Examples

The following example shows sample output for the **show ssg dial-out exclude-list** command:

```
Router# show ssg dial-out exclude-list

Exclude DNIS prefixes downloaded from profile exclude_dnis_aaa
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
ssg dial-out	Enters SSG dial-out configuration mode.

ssg dial-out

To enable the SSG L2TP Dial-Out feature and enter SSG dial-out configuration mode, use the **ssg dial-out** command in global configuration mode. To remove all SSG dial-out configurations, use the **no** form of this command.

ssg dial-out

no ssg dial-out

Syntax Description

This command has no arguments or keywords.

Defaults

The SSG L2TP Dial-Out feature is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)B	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Use this command to enter SSG dial-out configuration mode to configure the SSG L2TP Dial-Out feature. Use the **no** form of this command to remove all SSG L2TP Dial-Out configurations.

Examples

The following example shows how to enter SSG dial-out configuration mode:

```
Router(config)# ssg dial-out
Router(config-dial-out)#
```

Related Commands

Command	Description
dnis-prefix all service	Configures the dial-out global service.
download exclude-profile (ssg dial-out)	Downloads the DNIS exclusion list locally or from a AAA server.
exclude dnis-prefix	Configures the DNIS filter by adding a DNIS prefix to the DNIS exclusion list.
show ssg dial-out exclude-list	Displays information about the DNIS prefix profile and the DNIS exclusion list.

Appendix A

This appendix displays successful debug output for the SSG L2TP Dial-Out feature.

Successful User Logon Debug Output

```
Router# show debugging
PPP:
  PPP protocol negotiation debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on

SSG:
  SSG control path errors debugging is on
  SSG control path events debugging is on

00:40:34: SSG-CTL-EVN: Received cmd (1,john) from Host-Key 60.0.0.2:0
00:40:34: SSG-CTL-EVN: Add cmd=1 from Host-Key 60.0.0.2:0 into SSG control cmd queue.
00:40:34: SSG-CTL-EVN: Dequeue cmd_ctx from the cmdQ and pass it to cmd handler
00:40:34: SSG-CTL-EVN: Handling account logon for host 60.0.0.2:0
00:40:34: SSG-CTL-EVN: No auto-domain selected for user john
00:40:34: SSG-CTL-EVN: Authenticating user john.
00:40:34: SSG-CTL-EVN: Deleting SSGCommandContext::~SSGCommandContext

00:40:34: RADIUS: Pick NAS IP for uid=9 tableid=0 cfg_addr=0.0.0.0 best_addr=9.2.33.2
00:40:34: RADIUS/ENCODE(00000009): acct_session_id: 11
00:40:34: RADIUS(00000009): sending
00:40:34: RADIUS(00000009): Send to unknown id 21645/22 9.2.36.253:1645, Access-Request,
len 66
00:40:35: RADIUS:  authenticator 58 38 59 C1 6D 9D 83 8F - 85 A0 11 16 5D 93 00 7C
00:40:35: RADIUS:  User-Name           [1]   10  "john"
00:40:35: RADIUS:  User-Password       [2]   18  *
00:40:35: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:40:35: RADIUS:  Service-Type        [6]   6   Login                     [1]
00:40:35: RADIUS:  NAS-IP-Address      [4]   6   9.2.33.2
00:40:35: RADIUS: Received from id 21645/22 9.2.36.253:1645, Access-Accept, len 86
00:40:35: RADIUS:  authenticator DE D8 18 E7 E1 34 51 D2 - C2 61 A1 B3 66 C5 03 9A
00:40:35: RADIUS:  Vendor, Cisco       [26]  14
00:40:35: RADIUS:   ssg-account-info   [250] 8   "Nsoho0"
00:40:35: RADIUS:  Vendor, Cisco       [26]  18
00:40:35: RADIUS:   ssg-account-info   [250] 12  "Npassthru1"
00:40:35: RADIUS:  Vendor, Cisco       [26]  20
00:40:35: RADIUS:   ssg-account-info   [250] 14  "Ntunnel_l2tp"
00:40:35: RADIUS:  Vendor, Cisco       [26]  14
00:40:35: RADIUS:   ssg-account-info   [250] 8   "NsohoX"
00:40:35: RADIUS(00000009): Received from id 21645/22
00:40:35: SSG-CTL-EVN: Response is good
00:40:35: SSG-CTL-EVN: Creating radius packet
00:40:35: SSG-CTL-EVN: Radius packet AAA attributes: 259:6 259:10 259:12 259:6
00:40:35: SSG-CTL-EVN: Creating HostObject for Host-Key 60.0.0.2:0
00:40:35: SSG-CTL-EVN: HostObject::Reset
00:40:35: SSG-CTL-EVN: HostObject::InsertServiceList Nsoho0
00:40:35: SSG-CTL-EVN: HostObject::InsertServiceList Npassthru1
00:40:35: SSG-CTL-EVN: HostObject::InsertServiceList Ntunnel_l2tp
00:40:35: SSG-CTL-EVN: HostObject::InsertServiceList NsohoX
00:40:35: SSG-CTL-EVN: DoAccountLogon: ProfileCache is not Set.
00:40:35: SSG-CTL-EVN: Account logon is accepted [Host-Key 60.0.0.2:0, john]
00:40:35: SSG-CTL-EVN: Send cmd 1 to host 60.0.0.2. dst=10.76.86.90:43504
00:40:35: SSG-CTL-EVN: Activating HostObject for Host-Key 60.0.0.2:0
00:40:35: SSG-CTL-EVN: Resetting default host route
00:40:35: SSG-CTL-EVN: Adding of default route for the host is successful
00:40:35: SSG-CTL-EVN: Deleting SSGCommandContext::~SSGCommandContext
```

```
00:40:35: RADIUS/ENCODE(00000009): Unsupported AAA attribute timezone
00:40:35: RADIUS: Pick NAS IP for uid=9 tableid=0 cfg_addr=0.0.0.0 best_addr=9.2.33.2
00:40:35: RADIUS(00000009): sending
00:40:35: RADIUS(00000009): Send to unknown id 21645/23 9.2.36.253:1646,
Accounting-Request, len 88
00:40:35: RADIUS:  authenticator 4D 90 B6 A7 55 29 6D B3 - 5B 25 F9 FA 2B 0E 14 CD
00:40:35: RADIUS:  Acct-Session-Id     [44]  10  "0000000B"
00:40:35: RADIUS:  Framed-IP-Address   [8]   6   60.0.0.2
00:40:35: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:40:35: RADIUS:  Authentic           [45]  6   RADIUS                    [1]
00:40:35: RADIUS:  User-Name           [1]   10  "john"
00:40:35: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
00:40:35: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:40:35: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:40:35: RADIUS:  NAS-IP-Address      [4]   6   9.2.33.2
00:40:35: RADIUS:  Acct-Delay-Time     [41]  6   0
00:40:35: RADIUS: Received from id 21645/23 9.2.36.253:1646, Accounting-response, len 20
00:40:35: RADIUS:  authenticator F3 5B 6B BF 15 E3 BC A6 - 3E 20 B4 CB 37 40 06 BA
SSG# show ssg host
1: 60.0.0.2

### Active HostObject Count: 1

Successful Service Logon Debugs
Router# show debugging
.
.
.
00:41:15: SSG-CTL-EVN: Received cmd (11,soho0) from Host-Key 60.0.0.2:0
00:41:15: SSG-CTL-EVN: Add cmd=11 from Host-Key 60.0.0.2:0 into SSG control cmd queue.
00:41:15: SSG-CTL-EVN: Dequeue cmd_ctx from the cmdQ and pass it to cmd handler
00:41:15: SSG-CTL-EVN: Handling service logon for Host-Key 60.0.0.2:0
00:41:15: SSG-CTL-EVN: Locating the HostObject for Host-Key 60.0.0.2:0
00:41:15: SSG-CTL-EVN: Creating pseudo ServiceInfo for service: soho0
00:41:15: SSG-CTL-EVN: ServiceInfo: Init servQ and start new process for soho0
00:41:15: SSG-CTL-EVN: Profile not found locally
00:41:15: SSG-CTL-EVN: Allocate aaa_req_handle for authorization for: soho0
00:41:15: SSG-CTL-EVN: Non-blocking AAA authorization request for soho0 sent successfully
00:41:15: RADIUS: Pick NAS IP for uid=0 tableid=0 cfg_addr=0.0.0.0 best_addr=9.2.33.2
00:41:15: RADIUS(00000000): sending
00:41:15: RADIUS(00000000): Send to unknown id 21645/24 9.2.36.253:1645, Access-Request,
len 57
00:41:15: RADIUS:  authenticator DC 0A E1 28 83 19 49 82 - F5 05 52 E3 20 83 4F D3
00:41:15: RADIUS:  User-Name           [1]   7   "soho0"
00:41:15: RADIUS:  User-Password       [2]   18  *
00:41:15: RADIUS:  Service-Type        [6]   6   Outbound                  [5]
00:41:15: RADIUS:  NAS-IP-Address      [4]   6   9.2.33.2
00:41:15: RADIUS: Received from id 21645/24 9.2.36.253:1645, Access-Accept, len 214
00:41:15: RADIUS:  authenticator 4C 95 80 EF D9 B0 00 B2 - 25 1C AA 6E B4 79 28 8D
00:41:15: RADIUS:  Vendor, Cisco       [26]  10
00:41:15: RADIUS:   ssg-service-info   [251] 4   "TT"
00:41:15: RADIUS:  Vendor, Cisco       [26]  28
00:41:15: RADIUS:   ssg-service-info   [251] 22  "R170.0.0.1;255.0.0.0"
00:41:15: RADIUS:  Vendor, Cisco       [26]  35
00:41:15: RADIUS:   Cisco AVpair       [1]   29  "vpdn:ip-addresses=100.0.0.2"
00:41:15: RADIUS:  Vendor, Cisco       [26]  37
00:41:15: RADIUS:   Cisco AVpair       [1]   31  "vpdn:l2tp-tunnel-password=lab"
00:41:15: RADIUS:  Vendor, Cisco       [26]  29
00:41:15: RADIUS:   Cisco AVpair       [1]   23  "vpdn:tunnel-type=l2tp"
00:41:15: RADIUS:  Vendor, Cisco       [26]  31
00:41:15: RADIUS:   Cisco AVpair       [1]   25  "vpdn:tunnel-id=lns_l2x0"
00:41:15: RADIUS:  Vendor, Cisco       [26]  24
00:41:15: RADIUS:   Cisco AVpair       [1]   18  "vpdn:dout-type=2"
00:41:15: RADIUS(00000000): Unique id not in use
```

```
00:41:15: RADIUS(00000000): Received from id 21645/24
00:41:15: SSG-CTL-EVN: Response is good
00:41:15: SSG-CTL-EVN: Creating radius packet
00:41:15: SSG-CTL-EVN: Radius packet AAA attributes: 260:2 260:20 97:9 124:3 x239:3 229:8
00:41:15: SSG-CTL-EVN: Received AAA response for service(soho0) download
00:41:15: SSG-CTL-EVN: The service is tunnel service, checking for SSG profile
00:41:15: SSG-CTL-EVN: Assigning RADIUS attributes
00:41:15: SSG-CTL-EVN: Inactive ServiceInfo. Adding MD5 hash
00:41:15: SSG-CTL-EVN: ServiceProfile MD5: 8BAE-47B9-B282-A40E--3ED9-2AC1-D64C-12D9
00:41:15: SSG-CTL-EVN: ssg_create_tunnel_cef_tbl: Create global tunnel cef table
00:41:15: SSG-CTL-EVN: Tableid for SSG's VRF 1
00:41:15: Service Address List :
00:41:15: Addr:170.0.0.0 mask:255.0.0.0
00:41:15: SSG-CTL-EVN: Handling service(soho0) requests after the AAA reply, action
00:41:15: SSG-CTL-EVN: ssg_pending_request: taking up the unqueued request
00:41:15: SSG-CTL-EVN: User accessing dial-out service, DNIS = 4444007
00:41:15: SSG-CTL-EVN: Service(soho0)::AddRef(): ref after = 1
00:41:15: SSG-CTL-EVN: Service(soho0): Request enqueued service
00:41:15: SSG-CTL-EVN: Dequeue cmd_ctx from the cmdQ and pass it to cmd handler
00:41:15: SSG-CTL-EVN: Locating the HostObject for Host-Key 60.0.0.2:0
00:41:15: SSG-CTL-EVN: Checking service mode.
00:41:15: SSG-CTL-EVN: Creating ConnectionObject (60.0.0.2:0, soho0)
00:41:15: SSG-CTL-EVN: Service(soho0)::AddRef(): ref after = 2
00:41:15: SSG-CTL-EVN: Checking maximum service count.
00:41:15: SSG-CTL-EVN: ConnectionObject: setting DNIS number to = 4444007
00:41:15: SSG-VPDN-CTL-EVN: Request has been issued to SSG-VPDN module
00:41:15: SSG-CTL-EVN: Service(soho0)::Release(): ref before = 2
00:41:15: SSG-CTL-EVN: Deleting SSGCommandContext::~SSGCommandContext

00:41:15: SSG-VPDN-CTL-EVN: State changed from Idle -> Authorizing on event Request Tunnel
00:41:15: SSG-VPDN-CTL-EVN: State changed from Authorizing -> VPDN Connecting on event
Authorization Success
00:41:15: SSG-VPDN-CTL-EVN: Authorization succeeded, establishing the tunnel
00:41:15: SSG-VPDN-CTL-EVN: Create/Clone vaccess to negotiate PPP
00:41:15: Vi4 PPP: Phase is DOWN, Setup
00:41:15: SSG-VPDN-CTL-EVN: VPDN callback to intimate call status
00:41:15: SSG-VPDN-CTL-EVN:  Call Status: CONNECTED
00:41:15: SSG-VPDN-CTL-EVN: State changed from VPDN Connecting -> PPP Negotiating on event
VPDN
Connected
00:41:15: SSG-VPDN-CTL-EVN: Start PPP negotiations on vaccess
00:41:15: %LINK-3-UPDOWN: Interface Virtual-Access4, changed state to up
00:41:15: Vi4 PPP: Treating connection as a dedicated line
00:41:15: Vi4 PPP: Phase is ESTABLISHING, Active Open
00:41:15: Vi4 LCP: O CONFREQ [Closed] id 1 len 10
00:41:15: Vi4 LCP:    MagicNumber 0x0409F842 (0x05060409F842)
00:41:15: Vi4 LCP: I CONFREQ [REQsent] id 1 len 15
00:41:15: Vi4 LCP:    AuthProto CHAP (0x0305C22305)
00:41:15: Vi4 LCP:    MagicNumber 0x04382A1C (0x050604382A1C)
00:41:15: Vi4 LCP: O CONFACK [REQsent] id 1 len 15
00:41:15: Vi4 LCP:    AuthProto CHAP (0x0305C22305)
00:41:15: Vi4 LCP:    MagicNumber 0x04382A1C (0x050604382A1C)
00:41:15: Vi4 LCP: I CONFACK [ACKsent] id 1 len 10
00:41:15: Vi4 LCP:    MagicNumber 0x0409F842 (0x05060409F842)
00:41:15: Vi4 LCP: State is Open
00:41:15: Vi4 PPP: Phase is AUTHENTICATING, by the peer
00:41:15: Vi4 CHAP: I CHALLENGE id 3 len 28 from "CLIENT1"
00:41:15: RADIUS/ENCODE(00000000): sendauth, failing over
00:41:15: RADIUS/ENCODE(00000000): send packet; BEGIN
00:41:15: Vi4 CHAP: Using hostname from interface CHAP
00:41:15: Vi4 CHAP: Using password from interface CHAP
00:41:15: Vi4 CHAP: O RESPONSE id 3 len 29 from "john"
00:41:15: Vi4 LCP: I CONFREQ [Open] id 1 len 15
00:41:15: Vi4 LCP:    AuthProto CHAP (0x0305C22305)
```

```
00:41:15: Vi4 LCP:    MagicNumber 0x04382A71 (0x050604382A71)
00:41:15: Vi4 PPP: Phase is TERMINATING
00:41:15: Vi4 PPP: Phase is ESTABLISHING
00:41:15: Vi4 LCP: O CONFREQ [Open] id 2 len 10
00:41:15: Vi4 LCP:    MagicNumber 0x0409F89F (0x05060409F89F)
00:41:15: Vi4 LCP: O CONFACK [Open] id 1 len 15
00:41:15: Vi4 LCP:    AuthProto CHAP (0x0305C22305)
00:41:15: Vi4 LCP:    MagicNumber 0x04382A71 (0x050604382A71)
00:41:15: Vi4 LCP: I CONFACK [ACKsent] id 2 len 10
00:41:15: Vi4 LCP:    MagicNumber 0x0409F89F (0x05060409F89F)
00:41:15: Vi4 LCP: State is Open
00:41:15: Vi4 PPP: Phase is AUTHENTICATING, by the peer
00:41:15: Vi4 CHAP: I CHALLENGE id 4 len 28 from "CLIENT1"
00:41:15: RADIUS/ENCODE(00000000): sendauth, failing over
00:41:15: RADIUS/ENCODE(00000000): send packet; BEGIN
00:41:15: Vi4 CHAP: Using hostname from interface CHAP
00:41:15: Vi4 CHAP: Using password from interface CHAP
00:41:15: Vi4 CHAP: O RESPONSE id 4 len 29 from "john"
00:41:15: Vi4 CHAP: I SUCCESS id 4 len 4
00:41:15: Vi4 PPP: Phase is FORWARDING, Attempting Forward
00:41:15: SSG-CTL-EVN: SSG authorization for SSS is needed
00:41:15: SSG-CTL-EVN: SSG Hook during ppp authenticated stage needed
00:41:15: Vi4 PPP: Phase is ESTABLISHING, Finish LCP
00:41:15: Vi4 PPP: Phase is UP
00:41:15: Vi4 IPCP: O CONFREQ [Closed] id 1 len 10
00:41:15: Vi4 IPCP:    Address 0.0.0.0 (0x030600000000)
00:41:15: Vi4 IPCP: I CONFREQ [REQsent] id 1 len 10
00:41:15: Vi4 IPCP:    Address 190.0.0.1 (0x0306BE000001)
00:41:15: Vi4 IPCP: O CONFACK [REQsent] id 1 len 10
00:41:15: Vi4 IPCP:    Address 190.0.0.1 (0x0306BE000001)
00:41:15: Vi4 IPCP: I CONFNAK [ACKsent] id 1 len 10
00:41:15: Vi4 IPCP:    Address 5.0.0.20 (0x030605000014)
00:41:15: Vi4 IPCP: O CONFREQ [ACKsent] id 2 len 10
00:41:15: Vi4 IPCP:    Address 5.0.0.20 (0x030605000014)
00:41:15: Vi4 IPCP: I CONFACK [ACKsent] id 2 len 10
00:41:15: Vi4 IPCP:    Address 5.0.0.20 (0x030605000014)
00:41:15: Vi4 IPCP: State is Open
00:41:15: Vi4 IPCP: Install negotiated IP interface address 5.0.0.20
00:41:15: SSG-CTL-EVN: Processing IPCP up event from PPP (Virtual-Access4)
00:41:15: SSG-CTL-EVN: Link is not a downlink interface
00:41:15: SSG-VPDN-CTL-EVN: ###### PPP/IPCP success
00:41:15: Vi4 IPCP: Install route to 190.0.0.1
00:41:15: Vi4 IPCP: Add link info for cef entry 190.0.0.1
00:41:15: SSG-VPDN-CTL-EVN: State changed from PPP Negotiating -> Success on event PPP
Negotiated
00:41:15: SSG-VPDN-CTL-EVN: PPP negotiations succeded..tunnel/session established
00:41:15: SSG-CTL-EVN: ServiceLogonCallback: bringing state to UP
00:41:15: SSG-CTL-EVN: Set tunnel CEF table ID (1) on vaccess Virtual-Access4
00:41:15: Vi4 IPCP: Remove route to 190.0.0.1
00:41:15: Vi4 IPCP: Install route to 190.0.0.1
00:41:15: SSG-CTL-EVN: Send cmd 11 to host 60.0.0.2. dst=10.76.86.90:43509
00:41:15: SSG-CTL-EVN: Activating the ConnectionObject.

00:41:15: SSG-CTL-ERR: Upstream route - service record unavailable
00:41:15: SSG-CTL-EVN: ssg_add_upstream_route - successful
00:41:15: SSG-CTL-EVN:  Acct Start: local: user_name=john

00:41:15: SSG-CTL-EVN: GetConnClass NULL len 0
00:41:15: SSG-CTL-EVN: SSG: Accounting:: AddCiscoVSA
00:41:15: SSG-CTL-EVN:  SSG: Accounting:: AddCiscoVSA add serviceName=soho0
00:41:15: SSG-CTL-EVN:  AddCiscoVSA: add serviceUserName=john

00:41:15: SSG-CTL-EVN:  AddCiscoVSA: no adding V attr  pService 64296F74
```

```
00:41:15:  RADIUS: Pick NAS IP for u=0x63BA3284 tableid=0 cfg_addr=0.0.0.0
best_addr=9.2.33.2
00:41:15: RADIUS: ustruct sharecount=1
00:41:15: Radius: radius_port_info() success=1 radius_nas_port=1
00:41:15: SSG-CTL-EVN: ServiceLogonCallback: Accept Service logon
00:41:15: SSG-CTL-EVN: Deleting SSGCommandContext::~SSGCommandContext
00:41:15: RADIUS(00000000): Send to  id 21645/25 9.2.36.253:1646, Accounting-Request, len
88
00:41:15: RADIUS:  authenticator 7E 0C BF 9F 91 FA 88 62 - C9 5E 63 59 1A A0 00 0B
00:41:15: RADIUS:  NAS-IP-Address      [4]   6   9.2.33.2
00:41:15: RADIUS:  NAS-Port            [5]   6   0
00:41:15: RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
00:41:15: RADIUS:  User-Name           [1]   10  "john"
00:41:15: RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
00:41:15: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:41:15: RADIUS:  Acct-Session-Id     [44]  10  "00000003"
00:41:15: RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
00:41:15: RADIUS:  Framed-IP-Address   [8]   6   5.0.0.20
00:41:15: RADIUS:  Acct-Delay-Time     [41]  6   0
00:41:15: RADIUS: Received from id 21645/25 9.2.36.253:1646, Accounting-response, len 20
00:41:15: RADIUS:  authenticator E9 DB A7 F3 62 38 D6 4B - B6 EC 26 54 F3 AE 7B 01
00:41:16: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access4, changed state
to up
SSG# show ssg service
1: soho0

### Total ServiceInfoObject Count: 1
```